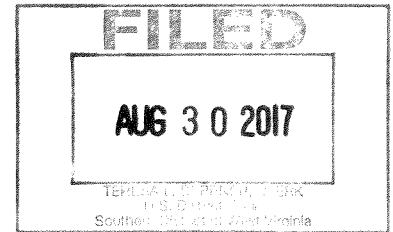


## UNITED STATES DISTRICT COURT

for the

Southern District of West Virginia

United States of America  
v.

Case No.

2:17-mj-00086

David Wayne McDaniel

Defendant(s)

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of October 8, 2016 in the county of Kanawha in the  
Southern District of West Virginia, the defendant(s) violated:

Code Section

Offense Description

18 USC 2252A(a)(2)

Attempted Distribution of Child Pornography

This criminal complaint is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.

Complainant's signature

Nicholas Ballance, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/30/2017City and state: Charleston, West Virginia

Judge's signature

Dwane L. Tinsley, United States Magistrate Judge

Printed name and title

A F F I D A V I T

STATE OF WEST VIRGINIA

COUNTY OF KANAWHA, to-wit:

I, Nicholas Ballance, being first duly sworn, do hereby depose and state as follows:

**BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), where I have been employed since June of 2016. I am a graduate of the FBI Training Academy in Quantico, Virginia where I received training in white collar crime, cyber-crime, interviewing, interrogation, evidence collection, intelligence analysis, and legal matters, among other topics.

2. I am currently assigned to the Charleston, West Virginia Resident Agency of the Pittsburgh Division. I am currently tasked with investigating violations of federal law such as child exploitation and child pornography, including, activity pertaining to the illegal production, receipt, distribution, and possession of child pornography in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.

3. Prior to joining the FBI, I served as a Deputy United States Marshal with the United States Marshals Service for a period of nine years. As part of my training, I attended the twelve week Criminal Investigator Training Program and six week Basic Deputy

United States Marshal Training at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also attended specialized law enforcement training in numerous topics such as fugitive investigations, sex offender investigations, financial investigations, and technical surveillance. I have also received training on the Child Protection System ("CPS") software. I have conducted several hundred fugitive investigations, utilizing state and federal court orders and search warrants to aide in locating violent fugitives.

4. This affidavit is intended only to show that there is sufficient probable cause for the complaint, and does not set forth all of your affiant's knowledge regarding the facts of this case.

**PEER-TO-PEER FILE SHARING**

5. Millions of computer users throughout the world use Peer-to-Peer ("P2P") file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

6. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a

user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a user downloading a file receives the entire file from one computer.

7. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular internet connection during an online session. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

8. P2P software users can search the P2P network by entering search terms into their P2P software to generate a list of available files that contain the search terms. For example, a person interested in obtaining child pornography images would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user then selects from the results the file(s) he/she wants to download. The files are downloaded directly

from the computer sharing the file. The downloaded files are stored in the area or directory previously designated by the user and/or the software. The downloaded files will remain in that same location until moved or deleted.

9. Law Enforcement can search the P2P networks to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. When a user on the P2P network offers a file to trade, the P2P software used by law enforcement calculates a "hash value" of the file using a SHA-1 hash. The Secure Hash Algorithm ("SHA") was developed by the National Institute of Standards and Technology, along with the National Security Agency, as a means of identifying files using a "digital fingerprint" that consists of a unique series of letters and numbers. A hash is a mathematical function that converts the data that comprises the contents of a file into an alphanumeric value. This value is unique to every file. A person may copy a file and rename it but if it is an exact copy, regardless of the name of the file, it will have the same hash value.

10. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. By comparing these hash values, one can determine whether two files are identical with a precision that greatly

exceeds 99.9999 percent certainty.

11. An investigator can examine the SHA-1 hash values of files being traded on the P2P network and determine if they are the same as the hash value of a file known to be child pornography. The investigator is able to do this by comparing the hash value associated with a file offered on the P2P network with hash values of movies or images of child pornography identified from previous investigations. The use of SHA-1 hash values for the matching of movies and images has proven to be extremely reliable. The investigator can then verify the contents of the file by viewing a copy of the file that has the same hash value from a library of known and/or suspected child pornography files kept by the investigator.

12. Most P2P programs allow users to designate specific folder(s) as "shared" folders. Any files contained in those specific folders are then made available for download by other users on the same P2P network. P2P software users typically do not "share" all of the files on their hard drive.

13. A Globally Unique Identifier ("GUID") is a 32-character alpha numeric sequence used in software applications. A GUID is produced when some P2P software applications are installed on a computer. The total number of unique keys is so large that the probability of the same number being generated twice is very small. By comparing GUIDs, it can be determined with a high degree of

certainty that two different IP addresses that have the same GUID are associated with the same computer. If one household has multiple computers, the GUID can be used to determine which computer in the household is sharing a particular file. Any user on the network can view the GUID of another user.

#### **BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE**

14. The Child Protection System ("CPS") is a software program designed to investigate the collection and distribution of child pornography by use of P2P software. The CPS software allows law enforcement to search P2P networks for files containing search terms or file names associated with child pornography. The CPS software has a geo-locate feature designed to limit the network search to the area of the investigator's authority. The CPS software generates a network activity spreadsheet. The spreadsheet contains information on certain files purported to be available from peers, as well as the IP address showing the locations of the material.

15. On October 12, 2016, Parkersburg Police Department Detective Travis Wolfe ("Det. Wolfe"), a member of the Violent Crimes Against Children Task Force ("VCACTF"), queried the CPS to obtain a list of IP addresses in West Virginia that were making available for distribution, known or suspected files containing child pornography, based on file hash values previously identified by law enforcement. On that same date, Det. Wolfe identified IP

address **50.110.254.226** as making 265 files, suspected to contain child pornography, available for download.

16. Your affiant reviewed a spreadsheet for IP address **50.110.254.226** which contained the following information: (a) the IP address for the target computer; (b) a time stamp referring to the date and time a file was available on the target computer; (c) the file's hash value; (d) the GUID; (e) the filename; (f) the file size; (g) the program being used for file sharing by the target; and (h) the percentage of the file available to download.

17. Your affiant did not download any of the 265 image files from the suspect IP address. Instead, your affiant reviewed copies of three video files found in the media library maintained by the West Virginia State Police that matched the SHA-1 hash values of those image files. The three files that depict child pornography, which CPS indicated were available for download on or about October 8, 2016, had the listed filenames on the target computer and are described as follows:



18.

File Name	File Description
11 and 13yo fuck daddy.mpg	A video that is 23 minutes and 28 seconds long showing two juvenile females performing multiple sexual acts to include both of the females undressing, one of the females exposing her vagina, one female straddling the other and rubbing her vagina on the other female's vagina, and one of the females having sexual intercourse with a male while the other female touches the adult male's penis and testicles.
Lolita Blowjob.avi	A video that is 3 minutes and 56 seconds showing a prepubescent female performing oral sex on an adult male until he ejaculates into her mouth.
Cp Tvg 13 Bond 10-11-12Yo Childlover Little Collection Video 0039 Girl- Vicky String Bikini Pthc 11Yo Pedofilia.mpg	A video that is 3 minutes and 23 seconds showing a prepubescent female with string wrapped around her chest. The prepubescent female is tied down and performs oral sex on an adult male.

19. A search of the American Registry for Internet Numbers ("ARIN") online database indicated that IP address **50.110.254.226** is registered to the Internet Service Provider (ISP) Frontier Communications of America ("Frontier"). On February 27<sup>th</sup>, 2017, your affiant served an administrative subpoena on Frontier

requesting subscriber records for IP address **50.110.254.226** for the time period of September 23<sup>rd</sup>, 2016 until October 8th, 2016. Frontier responded to the subpoena and advised that on the dates and times requested, IP address **50.110.62.93** was issued to Rick McDaniel, service address the same as the subject premises. Frontier indicated that the ISP activation date was July 12, 2013 and that service had been disconnected on December 7, 2016.

20. Your Affiant searched various records indices for information regarding Rick McDaniel located at 402 Ohio Avenue, Charleston, West Virginia 25302:

- a. Records from Kanawha County West Virginia indicate that the owner of 402 Ohio Avenue, Charleston, WV 25302 is Richard B. McDaniel.
- b. Records for 402 Ohio Avenue, Charleston, WV 25302 through various public record databases show it to be occupied by Richard Brian McDaniel, DAVID WAYNE MCDANIEL, and Elizabeth McDaniel.
- c. Records from the West Virginia Department of Motor Vehicles indicates 402 Ohio Avenue, Charleston, WV 25302 is utilized as the home address for Richard Brian McDaniel, DAVID WAYNE MCDANIEL, and Elizabeth Louise McDaniel.
- d. Records from the National Crime Information Center indicate that DAVID WAYNE MCDANIEL is currently a registered sex offender at 402 Ohio Avenue, Charleston, WV 25302. DAVID WAYNE MCDANIEL was convicted of two counts of 1<sup>st</sup> Degree Sexual Abuse on January 1<sup>st</sup>, 2006.

21. On July 5<sup>th</sup>, 2017, your affiant served an administrative subpoena on Suddenlink Communications, a known Internet Service Provider in the Charleston, West Virginia area, for any account

associated with 402 Ohio Avenue, Charleston, WV 25302. Suddenlink Communications responded to the subpoena and advised that there was an account registered to Richard McDaniel at this address and that the account activation date was December 7<sup>th</sup>, 2016.

22. On August 23, 2017, your affiant verified with the West Virginia State Police that DAVID WAYNE MCDANIEL is still registered with the sex offender registry as residing at 402 Ohio Avenue, Charleston, WV 25302.

23. On August 29, 2017, a federal search warrant was obtained for 402 Ohio Avenue, Charleston, West Virginia. The search warrant was executed at the residence on August 30, 2017. At the time the search warrant was executed, DAVID WAYNE MCDANIEL was present at the residence and agreed to talk to law enforcement. During this conversation, DAVID WAYNE MCDANIEL admitted to your affiant that he had used a P2P program, Shareaza, to download child pornography. DAVID WAYNE MCDANIEL further admitted that he knew he had images of child pornography available in a folder being shared with other users via Shareaza and he had observed that some of his files had been downloaded by other users.

24. DAVID WAYNE MCDANIEL also stated that he frequently deleted and reinstalled the Shareaza program. This information is consistent with the information obtained from the CPS program, which indicated that multiple GUIDs were identified as being connected to IP address **50.110.254.226** - each installation of

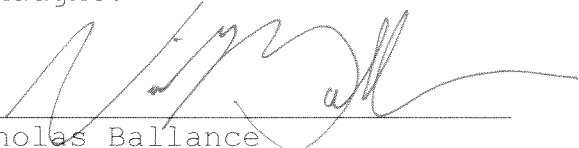
Shareaza generates a new GUID.

25. DAVID WAYNE MCDANIEL also stated that he stopped using Shareaza around October of 2016. This is consistent with the dates that CPS identified child pornography as being shared from IP address **50.110.254.226**, which was from approximately September 23, 2016 through October 8, 2016.

**CONCLUSION**

26. Your affiant respectfully submits that there is probable cause to believe DAVID WAYNE MCDANIEL, while located at or near Charleston, Kanawha County, West Virginia, and within the Southern District of West Virginia, knowingly attempted to distribute child pornography in and affecting interstate commerce by any means, including by computer, in violation of 18 U.S.C. § 2252A(a)(2), on or about October 8, 2016.

Further your affiant sayeth naught.

  
\_\_\_\_\_  
Nicholas Ballance  
Special Agent  
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence, this  
30th day of August 2017.

  
\_\_\_\_\_  
Dwane L. Tinsley  
United States Magistrate Judge